



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/824,985	04/15/2004	Kazuhiro Hara	450100-4879.1	7539
7590 03/06/2009 FROMMER LAWRENCE & HAUG LLP 745 FIFTH AVENUE NEW YORK, NY 10151			EXAMINER LAFORGLA, CHRISTIAN A	
			ART UNIT	PAPER NUMBER
			2439	
			MAIL DATE	DELIVERY MODE
			03/06/2009	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

**Office Action Summary****Application No.**

10/824,985

**Applicant(s)**

HARA, KAZUHIRO

**Examiner**

Christian LaForgia

**Art Unit**

2439

**Period for Reply** -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 09 January 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 20-39 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 20-39 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 25 January 2008 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☒ Certified copies of the priority documents have been received in Application No. 09/309,412.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SI/08)
- 4) ☐ Interview Summary (PTO-413)
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_
- Paper No(s)/Mail Date \_\_\_\_\_

**DETAILED ACTION**

1. The request for reconsideration of 09 January 2009 has been noted and made of record.
2. Claims 20-39 have been presented for examination.
3. Claims 1-19 and 40 have been cancelled as per Applicant's amendment.
4. Applicant's certified translation is also noted and made of record.

***Response to Arguments***

5. Applicant's arguments, see pages 2 and 3, filed 09 January 2009, with respect to the rejection of claims 20-39 under 35 U.S.C. 103 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new grounds of rejection is set forth below.

***Claim Rejections - 35 USC § 103***

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
7. Claims 20-24, 26-34, and 36-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,163,843 to Inoue et al., hereinafter Inoue, in view of U.S. Patent No. 7,100,020 B1 to Brightman et al., hereinafter Brightman.
8. As per claim 20, Inoue discloses a data transmission controlling method for controlling transmission of data from data transmitting means to data receiving means over communication channels and for causing said data transmitting means to encrypt data and transmit the encrypted data to said data receiving means over said communication channels, said data transmission controlling method comprising the steps of:

encapsulating the data to be transmitted in multiplexed fashion in accordance with a first protocol to form a section (Figures 12A-12D [Inner Protocols (IP/UDP/TCP)], column 12, lines 45-53, i.e. the inner protocols are encapsulated in an IP packet);

encrypting the section resulting from the encapsulation (Figure 12C [encrypted information], column 12, lines 45-53, i.e. as discussed below Section 3.2 of RFC 1825 describes encrypting the encapsulated data);

dividing the encrypted supplemented section into a plurality of payloads in accordance with a second protocol (Figures 12A-12D [leftmost IPv4 Header], column 12, lines 45-53, i.e. as discussed below Section 3.2 of RFC 1825 describes encapsulating the encrypted encapsulated data in a new cleartext IP header; RFC 1825 discusses fragmentation at Section 3.1; RFC 1826 discloses fragmentation in at least Section 1.1; RFC 1827 mentions fragmentation in Section 4); and

adding transport stream headers to each payload to form packets (Figures 12A-12D [Inner Protocols (IP/UDP/TCP)], column 12, lines 45-53, i.e. the inner protocols are encapsulated in an IP packet, which includes an IP header);

wherein the first encapsulating step is done before the encrypting step (column 12, lines 45-53, i.e. as discussed below Section 3.2 of RFC 1825 describes encapsulating prior to encrypting the encapsulated data) and the first protocol pads a portion of 0 to 63 bits (Figures 12B and 12C [Authentication Header (AH)], column 12, lines 45-53, i.e. RFC 1826 is incorporated into Inoue at column 12, line 47. RFC 1826 discloses at Section 3.2 (printed pages 5 and 6 of 13) that many implementations of the authentication header require padding up to 64 bits). Inoue discloses the use of the IP security standard and refers to RFC documents 1825-

1829. Printed pages 8 and 9 (of 21) of RFC 1825 (Section 3.2) provides more information regarding encapsulating an entire IP datagram or upper-layer protocols and encrypting that information before encapsulating it in a new cleartext IP header. Applicant is also directed to RFC documents 1826 (for information regarding the Authentication Header, abbreviated as AH in Inoue) and 1827 (for information regarding the Encapsulating Security Payload, abbreviated as ESP in Inoue) for information regarding encapsulation, encryption and padding. See MPEP § 2131.01 for the discussion on the use of multiple references.

9. Inoue does not teach supplementing the encrypted section with a section header and a section trailer, and wherein the padding is filled with a corresponding “1” as a suffix to the data.

10. It would have been obvious to one of ordinary skill in the art at the time the invention was made to fill the padding data with 1's and add it as a suffix to the data. Since it is padding data and is there to act as filler, it is irrelevant what data is actually used to fill the padding information. Inoue and the RFC documents disclose the Authentication Header as being in the middle of the datagram (see Figures 12B and 12C of Inoue). Relocating the Authentication header to the rear of the datagram, thereby making the padding data suffix information to the entire datagram, would have required only routine skill in the art since it has been held that the mere relocation of a part is not patently distinguishable if it has no bearing on the operation of the device. See MPEP § 2144.04; see *In re Japikse*, 181 F.2d 1019, 86 USPQ 70 (CCPA 1950).

11. Brightman discloses an encrypted payload (Figure 1 [element 121]) that is book-ended by a header (Figure 1 [element 129]) and trailer (Figure 1 [element 133], column 1, line 57 to column 2, line 13).

12. It would have been obvious to one of ordinary skill in the art at the time the invention was made to supplement the encrypted data section with a section header and trailer, since Brightman states at column 1, lines 57-60 that devices that deal with transport packets merely examine the header and trailer, thereby expediting the data through the network by eliminating the need to examine the encrypted information to route said data.

13. Regarding claims 21 and 22, Inoue discloses wherein said encapsulating in accordance with said first protocol supplements a real data part including said data to be transmitted to said data receiving means with an additional information part associated with said real data part and wherein said additional information part includes destination address information identifying the data receiving means authorized to receive data included in said real data part (Figure 12C [IPv4 header, middle of the packet], IPv4 headers include information such as source and destination address information).

14. Concerning claim 23, Inoue discloses wherein said destination address information is an individual (Figure 12C [IPv4 header, middle of the packet], IPv4 headers include information such as source and destination address information) or group destination address information (column 12, line 48, i.e. RFC 1825). Section 5.2 of RFC 1825 discloses using IPsec in a multicast type setting, thereby disclosing the group destination address information.

15. Concerning claim 24, Inoue discloses wherein said data transmitting means possesses session keys corresponding to said destination address information, said session keys being used

by said data transmitting means to encrypt information and data and by said receiving means to decrypt the encrypted information and data received; and wherein said data transmitting means transmits in advance said session keys to the data receiving means authorized to receive the transmitted information and data in accordance with said destination address information (column 12, line 48, i.e. RFC 1825). Section 4.4 of RFC 1825 discloses the use of different session keys for each client on the network.

16. Concerning claim 26, Inoue discloses wherein said session keys are transmitted over a communication channel permitting from said data transmitting means to said data receiving means or bidirectional communication therebetween (column 12, line 48, i.e. RFC 1825). Section 4.4 of RFC 1825 discloses how the different session keys are distributed.

17. With regards to claim 27, Inoue discloses wherein said encapsulating in accordance with said first protocol uniquely determines how said destination address information attached to said real data part is stored into said additional information part (column 12, lines 48, i.e. Section 3.2 of RFC 1825 describes encapsulating the data, see also RFC 1827), said encrypting step further encrypting said real data part using a master key specific to the data receiving means corresponding to said destination address information (column 12, line 48, i.e. RFC 1825). Section 4.4 of RFC 1825 discloses the use of different session keys for each client on the network.

18. Concerning claim 28, Inoue discloses wherein said additional information part provides a 48-bit space in which to accommodate said destination address information (Figures 12A-12D [IPv4 headers, Authentication Header]).

19. With regards to claim 29, Inoue wherein the communication channel is in a broadcast data transmission system, including a satellite broadcast system, and said encapsulating in accordance with said first protocol uniquely encapsulates the data to be transmitted to said data receiving means in accordance with either the Internet protocol (Figures 12A-12D [leftmost IPv4 Header], column 12, lines 45-53) or the Ethernet protocol.

20. Regarding claims 30-31, 36-37, Inoue discloses wherein said data receiving means is constituted as a bridge or an IP router (Figures 1 [blocks 4a, 4c], 2 [blocks 4a, 4b, 4c], 3, 6 [blocks 4a, 4b], column 7, lines 21-38).

21. As per claim 32, Inoue discloses a data transmission controlling method for controlling the transmission of data from data transmitting means to data receiving means over communication channels and for causing said data transmitting means to encrypt data and transmit the encrypted data to said data receiving means over said communication channels, said data transmission controlling method comprising the steps of:

encapsulating the data to be transmitted in multiplexed fashion in accordance with a first protocol to form a section (Figures 12A-12D [Inner Protocols (IP/UDP/TCP)], column 12, lines 45-53, i.e. the inner protocols are encapsulated in an IP packet), wherein the first protocol pads a



portion of 0 to 63 bits (Figures 12B and 12C [Authentication Header (AH)], column 12, lines 45-53, i.e. RFC 1826 is incorporated into Inoue at column 12, line 47. RFC 1826 discloses at Section 3.2 (printed pages 5 and 6 of 13) that many implementations of the authentication header require padding up to 64 bits);

encrypting the section using an encryption key (Figure 12C [encrypted information], column 12, lines 45-53, i.e. Section 3.2 of RFC 1825 describes encrypting the encapsulated data);

supplementing the encrypted section with encryption key information about said encryption key (Figure 12C [Key Information Header (Key)]);

dividing the encrypted supplemented section into a plurality of payloads in accordance with a second protocol (Figures 12A-12D [leftmost IPv4 Header], column 12, lines 45-53, i.e. as discussed below Section 3.2 of RFC 1825 describes encapsulating the encrypted encapsulated data in a new cleartext IP header; RFC 1825 discusses fragmentation at Section 3.1; RFC 1826 discloses fragmentation in at least Section 1.1; RFC 1827 mentions fragmentation in Section 4);

adding transport stream headers to each payload to form a packet (Figures 12A-12D [Inner Protocols (IP/UDP/TCP)], column 12, lines 45-53, i.e. the inner protocols are encapsulated in an IP packet, which includes an IP header);

transmitting said packets from said data transmitting means to said data receiving means (Figure 6, column 2, lines 57-64, column 6, line 64 to column 7, line 5); and

decrypting said packets using one of a plurality of decryption keys which allow said data receiving means to decrypt said encrypted data and which are updatable, said one of the decryption keys being selected in accordance with said encryption key information attached to

said encrypted data (column 6, line 64 to column 7, line 5, i.e. decryption is done according to the IPSec standards 1825-1827).

22. Inoue does not teach supplementing the encrypted section with a section header and a section tailer, and wherein the padding is filled with a corresponding “1” as a suffix to the data.

23. It would have been obvious to one of ordinary skill in the art at the time the invention was made to fill the padding data with 1’s and add it as a suffix to the data. Since it is padding data and is there to act as filler, it is irrelevant what data is actually used to fill the padding information. Inoue and the RFC documents disclose the Authentication Header as being in the middle of the datagram (see Figures 12B and 12C of Inoue). Relocating the Authentication header to the rear of the datagram, thereby making the padding data suffix information to the entire datagram, would have required only routine skill in the art since it has been held that the mere relocation of a part is not patently distinguishable if it has no bearing on the operation of the device. See MPEP § 2144.04; see *In re Japikse*, 181 F.2d 1019, 86 USPQ 70 (CCPA 1950).

24. Brightman discloses an encrypted payload (Figure 1 [element 121]) that is book-ended by a header (Figure 1 [element 129]) and trailer (Figure 1 [element 133], column 1, line 57 to column 2, line 13).

25. It would have been obvious to one of ordinary skill in the art at the time the invention was made to supplement the encrypted data section with a section header and tailer, since Brightman states at column 1, lines 57-60 that devices that deal with transport packets merely examine the header and trailer, thereby expediting the data through the network by eliminating the need to examine the encrypted information to route said data.

26. Regarding claim 33, Inoue discloses wherein said plurality of decryption keys include a decryption key which is currently usable for decrypting said encrypted data received, and a decryption key, encrypted data received; and wherein said data decrypting step selects the currently usable decryption key based on said encryption key information (column 12, line 48, RFCs 1825, 1826, 1827).

27. With regards to claim 34, Inoue discloses wherein said encryption key and said decryption keys are session keys for encrypting information and data (column 12, line 48, i.e. RFC 1825). Section 4.4 of RFC 1825 discloses the use of different session keys for each client on the network.

28. With regards to claims 38 and 39, Inoue teaches wherein said additional information part includes data to verify a communication channel (column 12, lines 43-52, i.e. Sections 1.3, 4.3, RFC 1825 discusses the Authentication Header ensures a trusted subnetwork and trusted communication channel).

29. Claims 25 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Inoue in view of Brightman as applied above, and in further view of U.S. Patent No. 6,178,244 B1 to Takeda et al., hereinafter Takeda.

30. Concerning claims 25 and 35, Inoue and Brightman do not teach a data transmission controlling, wherein said session keys are updated at predetermined intervals.

31. Takeda discloses a data transmission controlling, wherein said session keys are updated at predetermined intervals (column 12, lines 38-44).

32. It would have been obvious to one of ordinary skill in the art at the time the invention was made to update the session keys at predetermined intervals, since a skilled artisan would realize that it would improve security. By updating session keys at predetermined intervals, it makes it more difficult for an eavesdropper to crack encrypted sessions because the keys are constantly changing.

### ***Conclusion***

33. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

34. The following patents are cited to further show the state of the art with respect to encapsulating security payloads (ESP) headers and trailers, such as:

United States Patent No. 6,795,917 B1 to Ylonen, which is cited to show providing a header or trailer to an IPSec packet.

United States Patent No. 7,032,242 B1 to Grabelsky et al., which is cited to show ESP header and trailers, although there does not appear to be support in parent patent 6,353,614.

United States Patent No. 7,028,335 B1 to Borella et al., which is cited to show ESP header and trailers, although there does not appear to be support in parent patent 6,353,614.

United States Patent No. 6,055,236 to Nessett et al., which is cited to show ESP header and trailers, although there does not appear to be support in parent patent 6,353,614.

##. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792.

The examiner can normally be reached on Monday thru Thursday 7-5.

##. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

##. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/  
Primary Examiner, Art Unit 2439

clf